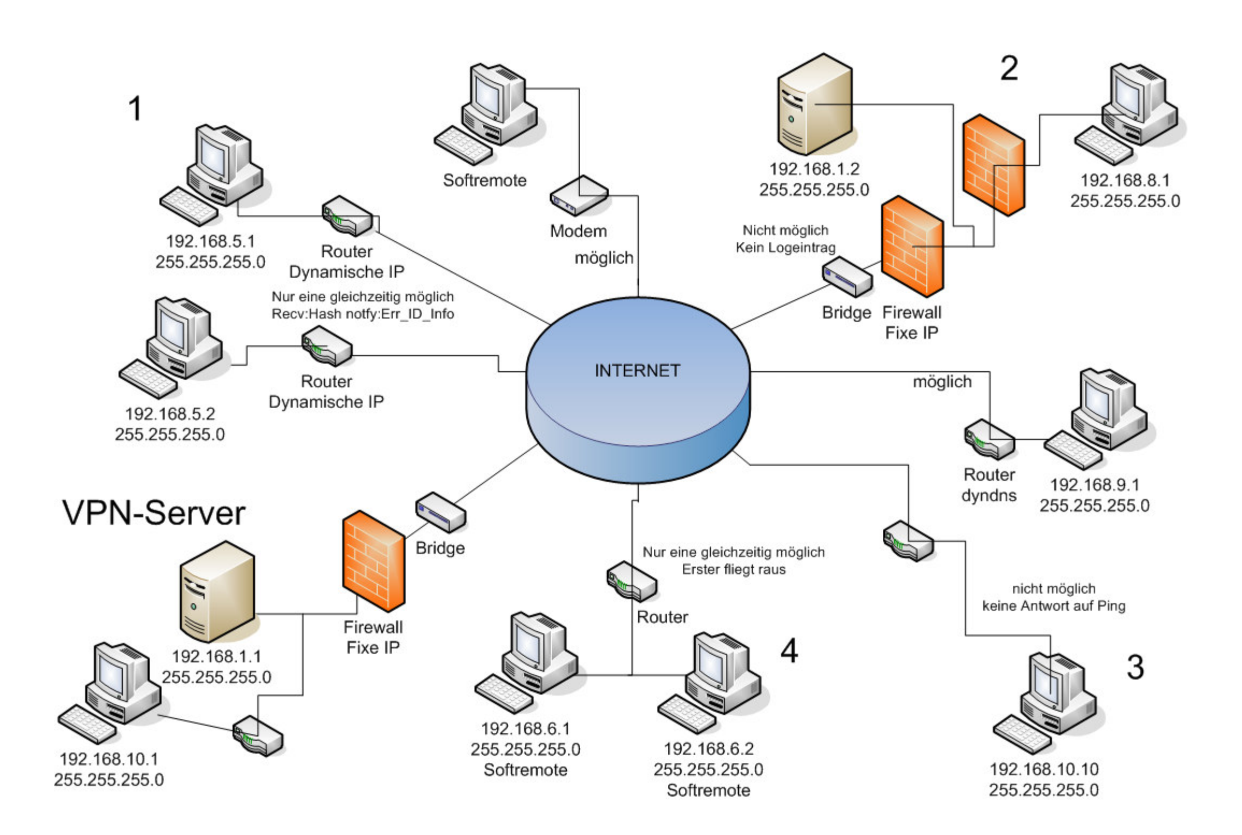
Dieses Dokument beschreibt die häufigsten Ursachen für VPN-Verbindungs-probleme.

Situationsplan

Das folgende Diagramm zeigt schematisch die verschiedenen Netzwerk-Situationen. Jedes der Netzwerke 1 bis 4 ist untereinander unabhängig zu betrachten. Es wird jeweils versucht eine Verbindung zum VPN-Server herzustellen.



Situation 1

Verhalten:	Es kann jeweils nur eines der Netzwerke einen VPN-Tunnel zum VPN-Server aufbauen. Das zweite Netzwerk kann den Tunnel nicht aufbauen.
Problem:	Die IP-Adressen 192.168.5.1 und 192.168.5.2. Beide Netze haben die gleiche Netz-ID.
Logeintrag:	Recv: Hash Notfy: ERR_ID_Info
Lösung:	Eines der Netzwerke muss seine Netz-ID ändern. Zum Beispiel auf 192.168.11.0.

Situation 2

Verhalten:	VPN-Tunnel wird nicht aufgebaut.
Problem:	Die DMZ hat die gleiche Netz-ID wie der VPN-Server.
Logeintrag:	Keiner, da die VPN-Anfrage nicht bis zur VPN-Firewall gelangt, sondern direkt in der DMZ landet.
Lösung:	Die Netz-ID der DMZ ändern. Zum Beispiel auf 192.168.12.0

Situation 3

Verhalten:	Der Tunnel wird zwar aufgebaut, aber man bekommt keine Antwort vom Ziel-Netz.
Problem:	Auf der Serverseite ist ebenfalls ein Netz 192.168.10.0 bekannt. Die ankommenden Päckchen werden über einen anderen Router wie-tergeleitet.
Logeintrag:	Keine Fehlermeldung.
Lösung:	Entweder die Client-Netz-ID ändern, oder die gleichnamige Netz-ID auf der Seite des VPN-Servers. Zum Beispiel auf 192.168.13.0.

Situation 4

Verhalten:	Einer der PCs kann über den Softremote Client einen VPN-Tunnel aufbauen. Wird versucht mit dem zweiten PC eine weitere VPN-Verbindung aufzubauen, wird die erste Verbindung getrennt.
Problem:	Das NAT des Routers. Beide Clients arbeiten mit Port 500. Der Router kann aber nur eine Session mit dem gleichen Port offen halten.
Logeintrag:	Keine Fehlermeldung.
Lösung:	Eine Hardwarelösung, welche das ganze Netzwerk unterstützt.

Logeinträge

NO_PROPOSAL_CHOSEN

- Der Encryption oder Hash Algorythmus stimmen nicht überein (Phase 1 oder 2).
- Die Perfect-Forward-Secrecy stimmt nicht überein.
- Der Negotiation-Mode stimmt nicht überein.

INVALID_ID_INFO oder ERR_ID_INFO:

- Die internen IP-Adressen unter Local oder Remote stimmen nicht überein.
- Der ID-Typ der öffentlichen IP Adressen oder die Adressen selbst sind falsch eingetragen.

Received malformed message or negotiation no longer active,
PYLD_MALFORMED oder PAYLOAD_MALFORMED:

- Die zwei Pre-Shared-Keys stimmen nicht überein. Auf beiden Seiten muss der gleiche Key eingetragen sein.

Message not received! Retransmitting!
IKE Retransmit!

- Ist die VPN-Rule auf 'active' gesetzt?
- Ist der IKE-Port 500 in der Firewall offen?
- Ist unter 'My IP' der VPN-Rule die öffentliche IP-Adresse richtig eingetragen?
- Nur ADSL: Ist der PPPoE-Link up (Nailed-Up Connection)?

Failed to resolve Secure Gateway

- Ist der DynDNS Name korrekt unter Secure Gateway eingetragen?
- Sind im LAN-Teil DNS-Server eingetragen?

FAQ

Wofür ist die Einstellung NAT-Traversal?

Sollte der VPN-Client hinter einem NAT-Router stehen, der nicht VPN-pass-through unterstützt, muss dies aktiviert werden. Die meisten aktuellen Router unterstützen aber VPN-pass-through.

Für was ist die Einstellung DNS-Server (for IPSec VPN)?

Dieser DNS-Server ist für die Namensauflösung der PCs, welche man per VPN sucht. Ein lmhosts-Eintrag ist nicht mehr nötig.

Für was ist die Einstellung Keep alive?

Normalerweise wird eine VPN-Verbindung getrennt, sobald für zwei Minuten keine Daten übertragen wurden. Mit dieser Einstellung bleibt der Tunnel bestehen.

Können zwei Netzwerke mit der gleichen Netz-ID über VPN verbunden werden?

Nein, VPN arbeitet mit Routing und braucht somit zwei verschiede Netz-IDs.

Knowledgebaseeinträge

Einige KB-Einträge zu diesem Thema. Sie finden weitere in unserer Knowledgebase.

1710 - Unterschiedliche SA Lifetime zwischen VPN-Tunnelendpunkten

Die VPN-Tunnelpunkte können unterschiedlich sein. Der erste, bei dem das SA Lifetime abgelaufen ist, sendet ein "delete SA request" zum Peer. Daraufhin wird der Tunnel neu aufgebaut.

1544 - VPN-Verbindung nur bei aktivem Internetzugriff

Damit die VPN-Verbindung jederzeit von aussen ausfgebaut werden kann, muss die Option **Nailed-Up-Connection** aktiviert werden. Dieser Parameter ist jedoch nur vorhanden, wenn die Firewall das PPPoE-Protokoll unterstützt.

1847 - VPN Zombie Tunnel

Sie müssen den chk_input Timer auf zwei Minuten einstellen. Somit geht der SA, wenn kein Incoming Traffic innerhalb von zwei Minuten kommt, down. Diese Einstellung verhält sich wie ein idle timeout für VPN:

Telnet-Menu 24.8 :

sys edit autoexec.net
i (für Insert)
ipsec timer chk_input 2
x (für Exit und Save)
sys r (Zywall 10 reboot)

1815 - Kein Ping über VPN-Tunnel

Falls bei aufgebautem Tunnel (siehe SA Monitor) auf Ping keine Antwort folgt, überprüfen Sie folgendes:

- Der Default-Gateway bei den PCs muss die entsprechende ZyWALL im eigenen LAN sein
- Auf den PCs muss jegliche Firewall-Software deaktiviert oder entsprechend konfiguriert sein
- Die Firewall von Bluewin darf nicht aktiv sein
- Falls auf der ZyWALL unter SUA/NAT alle Ports auf einen Server weitergeleitet werden, muss der Port 500 separat auf die LAN-Adresse der ZyWALL umgeleitet sein
- Die DMZ-IP-Adresse der Geräte darf nicht im gleichen IP-Range wie die Gegenstelle (Default IP 192.168.2.1) sein.

1911 - Keine VPN-Verbindung über die Swisscom Unlimited Card mit VPN Client

Bei der Verwendung einer VPN-Verbindung über die Swisscom Unlimited Card muss darauf geachtet werden, dass beim VPN Server der Betriebsmodus "**NAT Traversal**" ausgewählt ist.

Bei nicht aktiviertem "**NAT Traversal**" wird das Routing über das UMTS/GPRS/GSM nicht einwandfrei durchgeführt.

1539 - Kein Internetzugriff mehr, sobald PC mit VPN-Konfiguration im Netz

Wenn sich der PC mit installiertem und konfiguriertem SoftRemoteLT im gleichen Subnet befindet, auf welche sich auch eine VPN-Verbindung bezieht, muss entweder SoftRemoteLT manuell deaktivieren werden (mit rechter Maustaste auf Icon und deaktivieren) oder in der Definition der entsprechenden VPN-Verbindung von SoftRemote folgender Eintrag gesetzt werden: Only Connect Manually. Mit dieser Einstellung muss die VPN-Verbindung manuell aufgebaut werden.